CRYPTOGRAPHY BASED ON COMBINATORIAL MATRICES

A synopsis for the proposed Ph.D. Research work in Mathematics

Supervisor

Dr. Sheet Nihal Topno

Assistant Professor,

Department of Mathematics

Ranchi University, Ranchi

Research Scholar

Amit Ram Baraik

Submitted To

UNIVERSITY DEPARTMENT OF MATHEMATICS

FACULTY OF SCIENCE

RANCHI UNIVERSITY, RANCHI

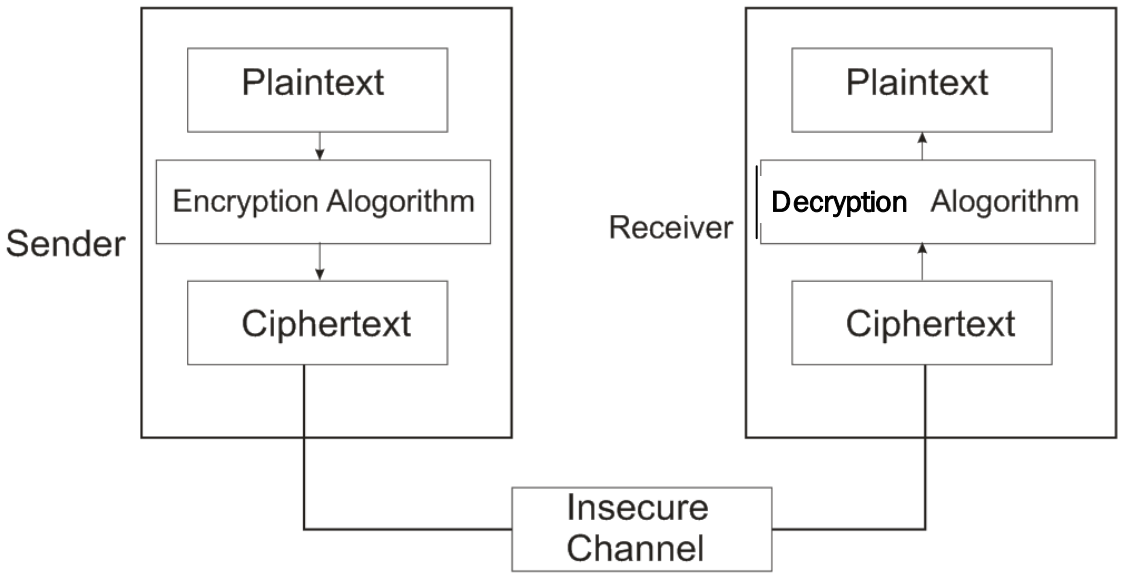
JHARKHAND

2023

1. State of the Art :

1.1 Origin of Cryptography :

Cryptosystems have been in practice since around 1900 B.C. The Study of cryptosystems and their strength are recent developments. This study is called cryptography in general. The word cryptography came from the Greek word kryptos+Graphein. kryptos means hidden and graphein means to write. So, cryptography is the art of hiding data with the help of some technique and that technique can be anything. It has been shown with the help of diagram below.



1.2 Some terms used in cryptography [1,4]:

Plaintext : A message to be sent is known as plaintext or the original form of the message is called plaintext.

Ciphertext : To prevent unauthorized access, plaintext is converted into a code and this transformed message is called ciphertext.

Encryption : The Process of converting plaintext to cipher text by using some technique is called encryption.

Decryption : The Process of converting encrypted message into original form is called decryption.

Key : Key is a secret information for encryption and decryption of the message in cryptography, which is shared between sender and receiver.

Hacker : An unauthorised cryptanalyst, that may be a person or a system is called a Hacker or Attacker.

1.3 Recent Advances in cryptography :

In the year 2019 M. Zeriouh et al. [3] used matrices for the encryption and decryption scheme. In this scheme the matrix K= $M_{k,l}$ is used as the seerete Key, where k, l $\in$ N*. The scheme gives $O(n^{lk})$ to calculate complexity. Where n is the size of the input.

In the year 2019 shipra Kumari et al. [5] proposed a method of encrypting and decryption based on conference matrix. This scheme requires a private key (p, r, r', d, q, p (p^r)), where p=odd prime, r is positive integer to encrypt or decrypt the message. A conference matrix A of order n, where gcd (n + 1, q) = 1 is used in the scheme. It's computational complexity is $O(2^{n^2})$.

In the year 2021, S.A. Farizi et al. [6] used Hadamard matrix in the construction of encryption and decryption scheme. In this scheme a simple Key is used which is written in matrix form and a Hadamard matrix of suitable order is applied.

In the year 2023 M. Kumari et al. [2] proposed public Key cryptography using recursive block matrices involving generalised Fibonacci numbers over a finite field Z_P. In this scheme Multinacci block matrices are used. This system comes with a large Key space and its security relies on the discrete Logarithm problem (D.L.P.).

2. Problem to be Investigated :

In this proposed research, we aim to develop cryptosystems using combinatorial matrices, which are not yet employed. Some of these

matrices are block structured Hadamard matrix, conference matrix weighing matrix and other incidence matrices of different designs.

Cryptanalysis is inevitable part of any cryptosystem, therefore it will also be done.

3. Objective of the Research :

In this era, exchange of data with proper security is the need of the present hour. Strong cryptosystems are supposed to be developed, since the old cryptosystems are on continuous attack. The objective of this research work is to contribute in this quest.

4. Tools to be used :

This research work will depend on the recent development in cryptography. For this, relevant books and journals are needed. To develop and test the cryptosystem and for cryptanalysis, mathematical software's like MATLAB will be used.

5. Contribution to the existing knowledge :

Various mathematical objects have been used to develop cryptosystems but, we aim to employ combinatorial matrices, which are in recent trend. Therefore this research work will surely contribute to the existing knowledge.

6. Need of the society :

The society needs exchange of data with privacy. Proposed research work aims to help the society in this area.

7. Conclusion :

The proposed research work will go through unknown path, but with the help of developed concepts and new idea we hope to complete this research work and contribute to the society.

References :

[1] D. R. Stinson, Cryptography theory and practice, *CRC Press Taylor & Francis Group*, LLC, third Indian Reprint, (2015).

[2] M. Kumari and J. Tanti, *Cryptography using multinacci block* matrices, Int. J. Nonlinear Anal. Appl. In Press, 1-9 http://dx.doi.org/10.22075/ijnaa.(2023).29918.4295

[3] M. Zeriouh, A. Chillali and *A. Boua, Cryptography based on the matrices,* Bal.soc. Paran. mat. (3s) v.373 (2019): 75-83. doi: 10.5269/bspm.v37i3.34542

[4] R. Bose, Information theory coding and cryptography, *Tata McGraw-Hill company limited*, (2005).

[5] S. Kumari and H. Mahato, *Encryption based on Conference matrix* arXiv: 1912.10757v1 [cs, CR] 23 Dec 2019.

[6] Salman Al Farizi, Mashuri Mashuri, Bambang Hendriya Guswanto, *Hadamard Matrix on Cryptographic Problems*, Advance in physics Research, volume 5, Soedirman International conference on mathematics and Applied Sciences (SICOMAS 2021)

Research Guide

Dr. Sheet Nihal Topno

Research Scholar

Amit Ram Baraik